

CLAIMS

What is claimed is:

1. A method for improving the security of software, comprising the steps of:

5 a) reading encrypted software from a non-volatile storage medium;

b) storing said encrypted software in a temporary storage medium; and,

10 c) decrypting those portions of said encrypted software that are read into an instruction cache in a processor as each of said portions is read into said instruction cache.

2. A method as described in Claim 1, wherein portions of said encrypted software not read into said instruction cache are left in an encrypted state.

15 3. A method as described in Claim 1, wherein said encrypted software comprises the steps of a computer program.

4. A method as described in Claim 1, wherein said temporary storage medium is computer RAM.

5. A method as described in Claim 1, wherein said step of decrypting said encrypted software portions is accomplished by a decryption unit located within said processor.

6. A method as described in Claim 1, wherein said step of  
5 decrypting said encrypted software portions is accomplished by a dedicated decryption device.

7. An apparatus for protecting the security of encrypted software, comprising:

10 a computer software non-volatile storage device for storing encrypted software;

a computer software temporary storage device for storing encrypted software, coupled with said computer software non-volatile storage device; and,

15 a processing device, coupled with said computer software temporary storage device, comprising an internal instruction cache and a decryption unit;

wherein said decryption unit is adapted to decrypt selected portions of said encrypted software as each of said portions is written to said instruction cache of said processing device.

8. An apparatus as described in Claim 7, wherein said non-volatile storage device is an optical storage device.

9. An apparatus as described in Claim 7, wherein said non-volatile storage device is a magnetic storage device.

5 10. An apparatus as described in Claim 7, wherein said non-volatile storage device is located remotely from said processor.

11. An apparatus as described in Claim 7, wherein said temporary storage device is computer RAM.

12. A system for protecting the security of encrypted software,  
10 comprising:

a) a computing device capable of receiving and storing software, said computing device further comprising:

a computer software non-volatile storage device;

a computer software temporary storage device, coupled  
15 with said computer software non-volatile storage device;  
and,

a processing device, coupled with said computer software temporary storage device, and comprising an instruction cache and a decryption unit;

- b) encrypted software, operable to be stored in said temporary software storage device;

wherein said decryption unit is adapted to decrypt encrypted software as said software is called to be written to said instruction  
5 cache of said processing device.

13. A system as described in Claim 12, wherein said decryption unit is implemented in a hardware device.

14. A system as described in Claim 12, wherein said decryption unit is implemented in software.

10 15. A system as described in Claim 12, wherein said encrypted software comprises the steps of a computer program.

16. A system as described in Claim 12, wherein said encrypted software comprises intellectual property intended to be processed by another computer program.